THREAT OF MALICIOUS CODE

The Department of Energy (DOE) is strongly committed to the protection of all DOE assets from cyber attack and malicious exploitation. This includes information, networks, hardware, software, and mobile devices.

DOE's continued diligence in this arena is critical in today's constantly–evolving cyber threat landscape. A recently cited incident involved senior officials receiving unsolicited free phone chargers. Luckily, the source was legitimate and did not result in a cyber incident, but it exemplifies how easily malicious code, also referred to as malware, can be covertly introduced in a computing environment via 'free' electronic or computing devices.

This threat is characterized by the delivery of a seemingly harmless component (CD/DVD, thumb drive, network component) to an unsuspecting user, and instructing the user to install the device. Depending on the intent of the malicious code embedded in the device, the component can damage or destroy files, computers, smart phones, and even agency networks.

If you receive a digital component or device from an unknown source, the device cannot be connected to DOE computers or networks. If you receive a device as a gift while in your official capacity at a DOE site, you should deliver the device and any packaging to your local security officer for examination and contact the DOE Joint Cybersecurity Coordination Center (JC3) circ@jc3.doe.gov.

Bob Brese is the CIO for the U.S. Department of Energy